RIGHT TO KNOW ADVISORY COMMITTEE
ENCRYPTION SUBCOMMITTEE

DRAFT AGENDA
July 16, 2012
9:00 a.m.
Room 438, State House, Augusta

Convene

1. Welcome and Introductions (Linda Pistner, Chair)

2. Presentations:
   Broadcasters (Suzanne Goucher, Maine Freedom of Information Coalition)
   Department of Public Safety (Lt. Colonel Ray Bessette)

3. Additional comments and discussion

4. Scheduling next meeting and agenda items

Adjourn

Maine Freedom of Information Coalition

PO Box 232
Augusta, Maine
04333

April 27, 2012

The Honorable David Hastings, Senate Chair
The Honorable Joan Nass, House Chair
Maine Right To Know Advisory Committee

Delivered via email

Dear Senator Hastings and Representative Nass:

An issue has come to our attention, and the members of the Maine Freedom of Information Coalition respectfully request that it be examined by the RTKAC when it reconvenes this summer.

The Federal Communications Commission has mandated that public safety agencies and other VHF and UHF land mobile spectrum users must migrate to narrower-bandwidth equipment by January 1, 2013. This shift is commonly known as "narrowbanding." In Maine, this migration, called MSCommNet, is being managed by the state Office of Information Technology. Among the features being touted for MSCommNet is the following: "Local Control - Each state agency will be able to decide who can listen and speak on their talk group and can assign their own security settings."[1]

It appears that public safety and other agencies in Maine and elsewhere are taking advantage of this "feature" by encrypting their radio transmissions[2], making it impossible for anyone to "listen in" on a conventional public-safety radio scanner. Indeed, this debate has been raging elsewhere since before 9/11/01[3], though it is relatively new to Maine.

While we recognize that there are legitimate public safety reasons for encrypting certain radio transmissions, such as for SWAT teams or hostage-response teams, we think a wholesale shift to

---

[1] Found at http://www.maine.gov/oit/services/radio/mscommnet/faq/MsCommNet_flyer.pdf

[2] For example, the Presque Isle police department has already migrated to an encrypted radio capability, with the Presque Isle fire department soon to follow. An encrypted system is also being used by the Caribou public works department. See http://www.mainemediaresources.com/ffj/02221201b.htm

[3] See, for example, "Police Scanners in the Digital Age," written in the summer of 2001, available at http://www.rtdna.org/pages/media_items/police-scanners-in-the-digital-age181.php

encryption of public safety radio transmissions raises several important freedom of information concerns:

- If such radio transmissions are encrypted, is it now, or will it become, illegal for members of the public to purchase scanners capable of decrypting them?
- If so, does this raise a concern that it has or will become illegal for citizens to monitor business conducted by public officials at public expense?
- What assurance will there be that the public will have access to the recordings, transcripts, or other public records of encrypted radio transmissions?
- What public safety concerns are raised by the inability of the news media to inform the public about breaking news or weather events that pose a risk to life or property if the media are unable to monitor public safety radio transmissions in real time?
- Is it possible to address the need for a limited amount of encryption capability by setting aside certain frequencies for this use, and keeping the remaining frequencies "in the clear"?

We offer the following in order to inform your discussion:

There is no HIPAA[4] implication in the move to encryption. HIPAA's health information privacy provisions apply only to "covered entities," which are defined in HIPAA rules[5] as follows:

> *Covered entity means:*
> *(1) A health plan.*
> *(2) A health care clearinghouse.*
> *(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.*

Public safety agencies, such as ambulance services, thus are not covered by HIPAA's privacy requirements.

There is nothing in the Federal Communications Commission's rules for the narrowbanding migration, or in the Federal Emergency Management Agency's grant guidance for funding for the migration, that requires a public safety agency to encrypt its radio transmissions. In fact, the U.S. Department of Homeland Security's SAFECOM Program has published on its website a document from the Public Safety Wireless Network Program, titled Security Issues Report—Impediments and Issues on Using Encryption on Public Safety Radio Systems, which reaches this conclusion:

> *The case for improved security in communications and system architecture through the use of encryption technologies still has not been made. Expense, coupled with the concern that less-than-ideal management resources and practices are available, remain significant reasons why radio system managers find it prohibitive to move encryption into their systems for consistently secured radio traffic.*

---

[4] The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
[5] 45 CFR 160.103, which can be viewed at http://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-sec160-103.pdf

The report is at http://tinyurl.com/cbe4wna[6].

In conclusion, we feel that "security" is not a suitable reason for public officials to draw the shade over an established source of sunshine. While many law enforcement agencies have argued that encrypted communications will keep their personnel safer and prevent criminals from monitoring their radio traffic, they have offered little hard evidence that those concerns outweigh the longstanding public interest in the openness of government activities. The secrecy that results from encrypted public safety information also impedes the public's right to know about matters of public concern and activities that are funded with public dollars.

We thank you for your attention to the foregoing, and for your exemplary service to the people of Maine.

Very truly yours,

Suzanne D. Goucher
President, MFOIC

[6] The full link is: http://www.safecomprogram.gov/SiteCollectionDocuments/Security_Issues_Report%20-%20Impediments_and_Issues_on_Using_Encryption_on_Public_Safety_Radio_Systems.pdf

State of Maine

DEPARTMENT OF PUBLIC SAFETY
OFFICE OF THE COMMISSIONER

PAUL R. LEPAGE
GOVERNOR

JOHN E. MORRIS
COMMISSIONER

SENT VIA E-MAIL

May 31, 2012

MAINE RIGHT TO KNOW ADVISORY COMMITTEE
Attn: The Honorable David R. Hastings III, Senate Chair
The Honorable Joan M. Nass, House Chair

SUBJECT: LAW ENFORCEMENT AND PUBLIC SAFETY AGENCIES' ENCRYPTED RADIO COMMUNICATIONS MATTER

Senator Hastings, Representative Nass:

I understand the Maine Right to Know Advisory Committee is creating a subcommittee to examine the concern recently raised by the Maine Freedom of Information Coalition regarding the imminent ability law enforcement and public safety agencies will have to digitally encrypt radio communications between such agencies.

Given the mission of the Maine Department of Public Safety, as well as the serious public safety, officer safety, and citizen privacy issues that would presumably be discussed in relation to this matter, I am respectfully requesting that at least one person from my department be appointed as an informal member to the Right to Know Advisory Committee's "Encryption Subcommittee" – this, to ensure that the multiple perspectives our agency has on this issue may be shared as the subcommittee and full committee consider this very important topic.

Respectfully,

JOHN E. MORRIS, COMMISSIONER
MAINE DEPARTMENT OF PUBLIC SAFETY

45 COMMERCE DRIVE, SUITE 1, 104 STATE HOUSE STATION, AUGUSTA, ME 04333-0104
TEL: (207) 626.3803 ▪ TTY: (207) 287.3659 ▪ FAX: (207) 287.3042